UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/590,898	08/28/2006	Kaoru Yokota	2006_1396A	4382

52349 7590 08/07/2009

WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER	
KING, CURTIS J	

ART UNIT	PAPER NUMBER
4147	

MAIL DATE	DELIVERY MODE
08/07/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/590,898	YOKOTA ET AL.	
	Examiner	Art Unit	
	CURTIS KING	4147	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 August 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 23 is rejected under 35 U.S.C. 101 because the claimed invention is not supported by either a process, manufacture and composition of matter, asserted utility or a well established utility.

Claim 23 claims "An authentication program for an authentication apparatus which permits a user to use a function provided by the authentication apparatus if authenticity of the user is certified by authentication, the authentication apparatus comprising: a tag verification information storage unit operable to store a plurality of pieces of tag verification information for identifying a plurality of wireless IC tags respectively, and the authentication program comprising the steps of: wirelessly receiving, from wireless IC tags attached to objects carried by the user, a plurality of pieces of tag certification information for identifying the wireless IC tags attached to the objects respectively; judging whether or not a level of match between the plurality of pieces of tag verification information and the plurality of pieces of tag certification information satisfies a predetermined condition; and permitting a use of the function if it is judged in the above step that the level of match satisfies the predetermined condition.". The software claimed as computer listings per see, i.e., the descriptions or expressions of the programs are not physical "things". They are neither computer components nor statutory process, as they are not "acts" being performed. Such

claimed computer program (software) does not define any structural and functional interrelationships between the computer program and other elements of a computer, which permit the computer program's functionality to be realized. As such, software (functional descriptive material) per se not claimed as embodied/encoded in computer-readable media is not statutory for that reason (i.e., "When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized"). Software by itself is not capable of causing functional change in the computer (transform underlying claimed subject matter to a different state or thing), nor machine (not tied to another statutory class, such as a particular apparatus), nor manufacture, nor composition of matter (i.e., tangible "thing") and therefore non-statutory.

Because the full scope of the claim as properly read in light of the disclosure encompasses non-statutory subject matter, the claim as a whole is non-statutory and appears to be one type of claim that is considered nonstatutory, under the present USPTO Interim Guidelines, 1300 Official Gazette Patent and Trademark Office 142 (Nov. 22, 2005).

Claim 23 also rejected under 35 U.S.C. 112, first paragraph. Specifically, since the claimed invention is not supported by either a process, manufacture and composition of matter, asserted utility or a well established utility for the reasons set

forth above, one skilled in the art clearly would not know how to use the claimed invention.

Claim 24 is rejected under 35 U.S.C. 101 because the claimed invention is not supported by either a process, manufacture and composition of matter, asserted utility or a well established utility.

Claim 24 claims "A computer-readable recording medium recording therein an authentication program that causes a computer to operate as an authentication apparatus which permits a user to use a function provided by the authentication apparatus if authenticity of the user is certified by authentication, the authentication apparatus comprising: a tag verification information storage unit operable to store a plurality of pieces of tag verification information for identifying a plurality of wireless IC tags respectively, and the authentication program comprising the steps of: wirelessly receiving, from wireless IC tags attached to objects carried by the user, a plurality of pieces of tag certification information for identifying the wireless IC tags attached to the objects respectively; judging whether or not a level of match between the plurality of pieces of tag verification information and the plurality of pieces of tag certification information satisfies a predetermined condition; and permitting a use of the function if it is judged in the above step that the level of match satisfies the predetermined condition." However, claim 24 does not clearly define a *computer-readable medium* to be a memory/disk, see Applicant's specification Page 164, lines 17-21 and is thus non-statutory for that reason.

Therefore, the full scope of claim 24 as properly read in light of the disclosure encompasses non-statutory subject matter,, i.e., signal, the claim as a whole is non-statutory, under the present USPTO Interim Guidelines, 1300 Official Gazette Patent and Trademark Office 142 (Nov. 22, 2005).

The Examiner suggests amending the claim *to include* the disclosed tangible computer readable media, while at the same time *excluding* the intangible media such as signals, carrier waves, etc...

Any amendment to the claim should be commensurate with its corresponding disclosure.

Claim 24 also rejected under 35 U.S.C. 112, first paragraph. Specifically, since the claimed invention is not supported by either a process, manufacture and composition of matter, asserted utility or a well established utility for the reasons set forth above, one skilled in the art clearly would not know how to use the claimed invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1, 2, 17, 19, 20, 21, and 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Ono (PG-Pub. No. 2004/0139020 A1).

In regard to claim 1, an authentication system (Ono fig. 1: 10) including a plurality of wireless IC tags (Ono fig. 1: 102a & ¶0036) and an authentication apparatus (Ono fig. 1: 200) which permits a user to use a function provided by the authentication apparatus if authenticity of the user is certified by authentication (Ono ¶0038 discloses the process unit performs a desired process after the user is authenticated), the authentication apparatus (Ono fig. 1: 200) comprising: a tag verification information storage unit (Ono fig. 2: 210 discloses as an Authentication Information Holding Unit) operable to store a plurality of pieces of tag verification information (Ono ¶0038 discloses as plurality of authentication information of each IC tag) for identifying the plurality of wireless IC tags respectively (Ono ¶0038); a receiving unit (Ono fig. 2: 230 & ¶0037 discloses the personal authentication unit serves also as an authentication information receiving unit; not shown but it's inherent) operable to wirelessly receive (Ono ¶0046, 0052 & 0057 discloses the personal authentication unit reads out the authentication information by radio from the IC tags), from wireless IC tags (Ono fig. 1: 102a) attached to objects (Ono fig. 1: 102 discloses as a portable article) carried by the user (Ono ¶0033), a plurality of pieces of tag certification information (Ono ¶0033 discloses tag certification information as authentication information & ¶0036 discloses the authentication apparatus can receive authentication information from a plurality of IC tags) for identifying the wireless IC tags (Ono fig. 1: 102a) attached to the objects (Ono fig. 1: 102) respectively (Ono fig. 3 & ¶0040 discloses the authentication holding unit holds the

names of the articles for authentication and the authentication of the IC tags); a tag judgment unit (Ono integrated in the personal authentication unit; not shown but it's inherent) operable to judge whether or not a level of match between the plurality of pieces of tag verification information and the plurality of pieces of tag certification information satisfies a predetermined condition (Ono ¶0046-0047); and a permission unit (Ono fig. 2: 230 discloses as a processing unit) operable to permit a use of the function if the tag judgment unit (Ono not shown but it's inherent) judges that the level of match satisfies the predetermined condition (Ono ¶0038 discloses the process unit performs a desired process using the individual information of the IC card after the personal authentication unit has certified the right person), and each of the plurality of wireless IC tags (Ono fig. 1: 102a & ¶0036) comprising: a tag certification information storage unit (Ono not shown but it's inherent) operable to store a piece of tag certification information (Ono discloses as authentication information) for identifying a wireless IC tag (Ono fig. 1: 102a) storing the piece of tag certification information (Ono ¶0033 discloses the IC tag holds an authentication information, thus, the IC tag must have a storage unit. Ono fig. 3: 210 & ¶0040 discloses authentication information identifying an article, hence, a IC tag); and an output unit (Ono not shown but it's inherent) operable to output wirelessly the piece of tag certification information (Ono ¶0033 the IC tag outputs the authentication information by radio, thus, the device inherently has an output unit).

In regard to claim 2, an authentication apparatus (Ono fig. 1: 200) which permits a user to use a function provided by the authentication apparatus (Ono fig. 1: 200) if authenticity of the user is certified by authentication (Ono ¶0038 discloses the process unit (fig. 2: 210 which part of the authentication apparatus unit) performs a desired process after the user is authenticated), the authentication apparatus (Ono fig. 1: 200) comprising: a tag verification information storage unit (Ono fig. 2: 210 discloses as an Authentication Information Holding Unit) operable to store a plurality of pieces of tag verification information (Ono fig. 3: shows a plurality of tag verification information for each article stored in the authentication information holding unit) for identifying a plurality of wireless IC tags respectively (Ono ¶0036 & fig. 3 discloses that a plurality of articles can be received by the authentication apparatus); a receiving unit (Ono fig. 2: 230 & ¶0037 discloses the personal authentication unit serves also as an authentication information receiving unit) operable to wirelessly receive (Ono ¶0046, 0052 & 0057 discloses the personal authentication unit reads out the authentication information by radio from the IC tags), from wireless IC tags (Ono fig. 1: 102a) attached to objects (Ono fig. 1: 102 discloses as a portable article) carried by the user (Ono ¶0033), a plurality of pieces of tag certification information (Ono ¶0046 discloses that the authentication information transmitted from the IC card and read by radio is identical with the authentication information selected from the authentication information holding unit, hence, it's obvious the IC card has a plurality of pieces of tag certification information) for identifying the wireless IC tags (Ono fig. 1: 102a) attached to the objects (Ono fig. 1: 102) respectively (Ono fig. 3 & ¶0040 discloses the authentication holding

unit holds the names of the articles for authentication and the authentication of the IC tags); a tag judgment unit (Ono integrated in the personal authentication unit; not shown but it's inherent) operable to judge whether or not a level of match between the plurality of pieces of tag verification information and the plurality of pieces of tag certification information satisfies a predetermined condition (Ono ¶0046-0047); and a permission unit (Ono fig. 2: 230 discloses as a processing unit) operable to permit a use of the function if the tag judgment unit (Ono not shown but it's inherent) judges that the level of match satisfies the predetermined condition (Ono ¶0038 discloses the process unit performs a desired process using the individual information of the IC card after the personal authentication unit has certified the right person).

In regard to claim 17, the authentication apparatus of claim 2, wherein each of the plurality of pieces of tag certification information contain a type code (Ono fig. 3: authentication information) indicating a type of an object to which a wireless IC tag identified by the piece of tag certification information is attached (Ono fig. 3 & ¶0046 discloses that the authentication information indicate the article the IC tag is attached to), wherein the tag judgment unit (Ono not shown but it's inherent) judges whether or not a level of match between the plurality of pieces of tag verification information (Ono: authentication information) and one or more pieces of tag certification information (Ono ¶0046-0047), which remain after excluding, from the plurality of pieces of tag certification information received by the receiving unit (Ono fig. 2: 230), pieces of tag certification information that contain a predetermined type code, satisfies a

predetermined condition (Ono ¶0044-0048 discloses the authentication apparatus uses weight coefficients of the tags to authenticate a user, hence, these weight coefficients are summed up and have to be greater than the reference value).

In regard to claim 19, the authentication apparatus of claim 2, wherein the tag judgment unit (Ono not shown but it's inherent) judges whether or not a ratio of (i) a number of pieces of tag verification information that, among the plurality of pieces of tag verification information, match any of the plurality of pieces of tag certification information to (ii) a total number of the plurality of pieces of tag verification information stored in the tag verification information storage unit (Ono fig. 2: 210) is equal to or higher than a standard value (Ono fig. 6 & ¶0049-0053 discloses that the authentication system can authenticate the user by the IC card and the number of authentication articles, thus, it would be obvious at the time of the invention to authenticate a user by comparing the number of received authentication articles(IC tags) to the number of tags in the storage unit to a predetermined value).

In regard to claim 20, the authentication apparatus of claim 2, wherein the tag verification information storage unit (Ono fig. 2: 210) further stores point values (Ono fig. 3: weight coefficients) indicating weights assigned to the plurality of pieces of tag verification information (Ono ¶0041), in correspondence with the plurality of pieces of tag verification information (Ono ¶0041 discloses that the weight correspond to the authentication information (tag verification information)), and the tag judgment unit (Ono

not shown but it's inherent) judges whether or not a ratio of (i) an acquired point value that is obtained by adding up point values corresponding to pieces of tag verification information (Ono: authentication information) that, among the plurality of pieces of tag verification information (Ono: authentication information), match any of the plurality of pieces of tag certification information to (ii) a total point value that is obtained by adding up point values corresponding to the plurality of pieces of tag verification information (Ono: authentication information) stored in the tag verification information storage unit (Ono fig. 2: 210) is equal to or higher than a standard value (Ono 0052-0053 discloses that the weight coefficients (point value) are added up and compared to a reference value (total point value) and certifies the right person when the value is greater than the set reference number).

In regard to claim 21, the authentication apparatus of claim 2, wherein the tag verification information storage unit (Ono fig. 2: 210) is a portable recording medium (Ono fig. 9 & 0061 discloses that the IC card can integrate into the IC card the authentication information holding unit from fig. 2: 210, thus, it's inherent to swap the storage unit out of the authentication apparatus and place it in the IC card), and the portable recording medium is inserted in the authentication apparatus (Ono fig. 1: 100 discloses the IC card (portable recording medium) being inserted into the authentication apparatus).

In regard to claim 22, claim 22 the method claim is analyzed with respect to claim 1 the system claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 3 & 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Shinzaki (Pat. No. 7,007,298 B1).

In regard to claim 3, Ono discloses the authentication of claim 2.

Ono does not disclose the authentication apparatus comprising an identification information storage unit operable to store first identification information, and a user judgment unit operable to, if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, receive second identification information and judge whether or not the first identification information matches the received second identification information, wherein the permission unit permits the use of the function if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, and if the user judgment unit judges that the first identification information matches the received second identification information.

Shinzaki discloses authentication apparatus comprising an identification information storage unit (Shinzaki fig. 6: discloses as password information registration and storage unit) operable to store first identification information (Shinzaki discloses as password col. 12 lines 1-2), and a user judgment unit (Shinzaki fig. 6: password information matching check unit) operable to judge if the level of match does not satisfy the predetermined condition (Shinzaki fig. 7: S24 & col. 12 lines 36-40), receive second identification information (Shinzaki fig. 7: S30 discloses request user to input password) and judge whether or not the first identification information matches the received second identification information (Shinzaki fig. 7: S33 & col. 12 lines 2-5). Once the authentication system authenticates the user at step S36, the user is allowed to use a function.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono authentication apparatus with Shinzaki password storage unit, as taught by Shinzaki. The combination of Ono in view of Shinzaki would yield to the claim limitation of "if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, receive second identification information and judge whether or not the first identification information matches the received second identification information, wherein the permission unit permits the use of the function if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, and if the user judgment unit judges that the first identification information matches the received second identification information".

The motivation would be to provide an additional feature to the user, for example, if the user did not have his/her wireless tag the user has the option to input a password to access the device.

In regard to claim 4, Ono in view of Shinzaki further discloses the authentication apparatus of claim 3, wherein the first identification information is either (i) first character information being a combination of one or more numerals and/or one or more alphabets and/or one or more signs or (ii) first biological information indicating biological characteristics of the user (Shinzaki col. 11 lines 21-34), the second identification information is either (i)second character information being a combination of one or more numerals and/or one or more alphabets and/or one or more signs or (ii) second biological information indicating biological characteristics of the user (Shinzaki col. 11 lines 21-34), if the user judgment unit receives the second character information, the user judgment unit judges whether or not the first character information matches the received second character information, and if the user judgment unit receives the second biological information, the user judgment unit judges whether or not the first biological information and the received second biological information correspond to a same user (Shinzaki fig. 7: S29-S33 & col. 11 lines 21-34).

3. Claims 5, 8, 13 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Ogawa (PG-Pub No. 2005/0027990 A1).

In regard to claim 5, Ono discloses the authentication apparatus of claim 2, wherein the plurality of pieces of tag verification information are a plurality of verification ID codes (Ono fig. 3: shows that the tag verification information are ID codes (i.e., authentication information & weight coefficients)) for identifying the plurality of wireless IC tags respectively (Ono fig. 3 shows the authentication information (i.e., 1125) stored in the authentication apparatus 200 authentication information holding unit 210 is used to identify the IC tags (i.e., 1125 identifies glasses)), the plurality of pieces of tag certification information are a plurality of certification ID codes (Ono ¶0046 discloses that the authentication information read by radio is identical with the authentication information selected from the authentication information holding unit (see fig. 3 for the information contained in the authentication information holding unit), thus, the certification ID codes is disclose as the authentication information & weight coefficients) for identifying the wireless IC tags (Ono fig. 1: 102a) attached to the objects respectively (Ono fig. 3 & ¶0041 it's obvious that the authentication information stored in the tag are codes (i.e., fig. 3: article 1125) that is used to identify the IC tags).

Ono does not disclose the authentication apparatus further comprises an update unit operable to, if a predetermined condition for update is satisfied, acquire at least two certification ID codes out of the plurality of certification ID codes received by the receiving unit, and update contents of the tag verification information storage unit by storing the at least two acquired certification ID codes into the tag verification information storage unit as verification ID codes.

Ogawa discloses an authentication apparatus that comprises an update unit (Ogawa fig. 4: 405 discloses as an updating section) operable to, if a predetermined condition for update is satisfied (Ogawa ¶0080 & 0085 discloses generating section 420 generates a symbol string which is the condition needed for the updating section to store the presentation string), acquire at least two codes (Ogawa ¶0094 discloses updating section receives a transformation result and presentation symbol string), and update contents of the storing section by storing (Ogawa fig. 4: 405 & 403 & 0094 discloses the updating section has the storing section store the transformation result and presentation symbol string) the at least two acquired codes into the storing section.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono in view of Ogawa authentication apparatus with an update unit, as taught by Ogawa. The combination of Ono in view of Ogawa would yield to the claim limitation "acquire at least two certification ID codes out of the plurality of certification ID codes received by the receiving unit, and update contents of the tag verification information storage unit by storing the at least two acquired certification ID codes into the tag verification information storage unit as verification ID codes".

The motivation would be to have an option to update a user authentication device tags associated with the user.

In regard to claim 8, Ono in view Ogawa further discloses the authentication apparatus of claim 5, wherein each of the plurality of certification ID codes (Ono fig. 3: authentication information & weight coefficients) contains a type code (Ono fig. 3:

authentication information (e.g., 1125)) indicating a type of an object to which a wireless IC tag (Ono fig. 1: 102a) identified by the certification ID code is attached (Ono ¶0046 discloses that the authentication information read by radio is identical with the authentication information selected from the authentication information holding unit (see fig. 3 for the information contained in the authentication information holding unit), thus, it's obvious the authentication information (certification ID codes) contain a type code (glasses) and the authentication information code (i.e.,) corresponds to that article (glasses see fig. 3)), wherein the update unit (Ogawa fig. 4: 405) acquires at least two (Ogawa fig. 4: 405 & 403 & 0094 discloses the updating section receives the transformation result and presentation symbol string) certification ID codes containing a predetermined type code (Ono fig. 3: authentication information column shows the predetermined type code for each article), from the plurality of certification ID codes received by the receiving unit (Ono fig. 2: 230).

In regard to claim 13, Ono discloses the authentication apparatus of claim 2, wherein the plurality of pieces of tag verification information are a plurality of pieces of unique authentication data for verification (Ono fig. 3 shows in the authentication holding unit a plurality of unique authentication data (authentication information and weight coefficients)) assigned by the authentication apparatus (Ono ¶0040), the plurality of pieces of tag certification information are a plurality of pieces of unique authentication data for certification assigned by the authentication apparatus (Ono ¶0046 discloses that the authentication information read by radio is identical with the authentication

information selected from the authentication information holding unit (see fig. 3 for the information contained in the authentication information holding unit), thus, the plurality of pieces of unique authentication data is disclose as the authentication information & weight coefficients), the receiving unit (Ono fig. 2: 230) wirelessly receives (Ono ¶0046, 0052 & 0057 discloses the personal authentication unit reads out the authentication information by radio from the IC tags), from the wireless IC tags (Ono fig. 1: 102a) attached to the objects (Ono fig. 1: 102 discloses as a portable article), a plurality of ID codes for identifying the wireless IC tags attached to the objects respectively (Ono ¶0036). Ono further discloses that the device comprises a transmission unit (Ono not shown but it's inherent) operable to transmit a signal to a wireless IC tag having an ID code corresponding to the piece of authentication data for verification (Ono ¶0046 discloses that the authentication apparatus transmits a signal to the IC tags corresponding to the article it is associated with).

Ono does not disclose the authentication apparatus further comprises an update unit operable to, if a predetermined condition for update is satisfied, generate a different piece of authentication data for each ID code received by the receiving unit, acquire at least two pieces of authentication data from pieces of generated authentication data, and update contents of the tag verification information storage unit by storing the at least two pieces of acquired authentication data into the tag verification information storage unit as authentication data for verification, and a transmission unit operable to transmit, for each piece of authentication data for verification having been updated by the update unit, a piece of authentication data for verification as a piece of

authentication data for certification, to a wireless IC tag having an ID code corresponding to the piece of authentication data for verification.

Ogawa discloses authentication apparatus comprising an update unit (Ogawa fig. 4: 405 discloses as an updating section) operable to, if a predetermined condition for update is satisfied (Ogawa ¶0080 & 0085 discloses generating section 420 generates a symbol string which is the condition needed for the updating section to store the presentation string) acquire at least two pieces of data of generated data (Ogawa ¶0094 discloses updating section receives a transformation result and presentation symbol string), and update contents of the storage section by storing the at least two pieces of acquired data into the storage section to be use for authentication (Ogawa fig. 4: 405 & 403 & ¶0094-0096 discloses the updating section has the storing section store the transformation result and presentation symbol string).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono authentication apparatus to include an update unit in order update coded information for the device, as taught by Ogawa. The combination of Ono in view of Ogawa would yield to the claim limitation " the authentication apparatus further comprises an update unit operable to, if a predetermined condition for update is satisfied, generate a different piece of authentication data for each ID code received by the receiving unit, acquire at least two pieces of authentication data from pieces of generated authentication data, and update contents of the tag verification information storage unit by storing the at least two pieces of acquired authentication data into the tag verification information storage unit as authentication data for verification, and a

transmission unit operable to transmit, for each piece of authentication data for verification having been updated by the update unit, a piece of authentication data for verification as a piece of authentication data for certification, to a wireless IC tag having an ID code corresponding to the piece of authentication data for verification".

The motivation would be to provide an addition security feature to a user, for example, there is a high possibility that data may be stolen when transmitted wirelessly this would improve and insure a safe authentication by the device (Ogawa ¶0007-0009).

In regard to claim 16, Ono in view of Ogawa further discloses the authentication apparatus of Claim 13, wherein each of the plurality of ID codes contains a type code (Ono fig. 3: discloses as authentication information) indicating a type of an object to which a wireless IC tag identified by the ID code is attached (Ono fig. 1: 102a & fig. 3 shows that the tag attached to the glasses has a code in the authentication table that is associated with the article column). Ono in view of Ogawa combination would yield to the claim limitation "wherein the update unit acquires at least two pieces of authentication data corresponding to ID codes that include a predetermined type code among the plurality of ID codes received by the receiving unit (Ogawa ¶0094 discloses updating section receives a transformation result and presentation symbol string)".

4. Claim 6, 9, 11 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Ogawa (PG-Pub No. 2005/0027990 A1) and further in view of Shinzaki (Pat. No. 7,007,298 B1).

In regard to claim 6, Ono in view of Ogawa discloses the authentication apparatus of claim 5, the predetermined condition for update (Ogawa ¶0080 & 0085 discloses the predetermined condition as the generating section 420 generates a symbol string which is the condition needed for the updating section to store the presentation string) and the update unit (Ogawa fig. 4: 405).

Ono in view of Ogawa does not disclose the authentication apparatus comprising an identification information storage unit operable to store first identification information, a user judgment unit operable to receive second identification information and judge whether or not the first identification information matches the received second identification information, and wherein the predetermined condition for update is that the first identification information matches the second identification information, and the update unit updates the contents of the tag verification information storage unit if the first identification information matches the second identification information.

Shinzaki discloses an authentication apparatus comprising an identification information storage unit (Shinzaki fig. 6: discloses as password information registration and storage unit) operable to store first identification information (Shinzaki discloses as password col. 12 lines 1-2), and a user judgment unit (Shinzaki fig. 6: password information matching check unit) operable to receive second identification information (Shinzaki fig. 6: 44 to 42) and judge whether or not the first identification information matches the received second identification information (Shinzaki fig. 7: S33 & col. 12 lines 2-5 & 46-50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono in view of Ogawa authentication apparatus to include an identification storage and user judgment unit to additionally verify a user, as taught by Shinzaki. The combination of Ono in view of Ogawa and Shinzaki would yield to the claim limitation "wherein the predetermined condition for update is that the first identification information matches the second identification information, and the update unit updates the contents of the tag verification information storage unit if the first identification information matches the second identification information".

The motivation would be to provide an additional feature to the user, for example, if the user did not have his/her wireless tag the user has the option to input a password to access the device.

In regard to claim 9, Ono in view of Ogawa discloses the authentication apparatus of claim 8 further comprising a priority level storage unit (Ono fig. 3 & ¶0048 Authentication Information Holding Unit Weight Coefficients Column discloses each article is given certain weights) operable to store a plurality of priority levels (Ono fig. 3: Weight Coefficients) with a plurality of type codes corresponding thereto (Ono fig. 3: shows the Authentication information corresponding to the Weight Coefficients), wherein the predetermined type code is correlated with priority levels (Ono ¶0048) that are less than or equal to a priority-level threshold value (Ono fig. 4: Reference Value & ¶0048 discloses the reference value which is the value that all of the articles weight coefficients need to add up to in order for the user to be allowed the function of the

authentication apparatus), and the update unit (Ogawa fig. 4: 405) acquires at least two (Ogawa fig. 4: 405 & 403 & 0094 discloses the updating section receives the transformation result and presentation symbol string) certification ID codes that have priority levels (Ono fig. 3: Weight Coefficient column) that are equal to or less than the priority-level threshold value (Ono fig. 3 & 4 ¶0048 discloses the reference value which is the value that all of the articles weight coefficients need to add up to in order for the user to be allowed the function of the authentication apparatus), from the plurality of certification ID codes received by the receiving unit (Ono fig. 2: 230)

Ono in view of Ogawa does not disclose wherein the predetermined type code is correlated with priority levels that are equal to or higher than a priority-level threshold value, and the update unit acquires at least two certification ID codes that have priority levels that are equal to or higher than the priority-level threshold value, from the plurality of certification ID codes received by the receiving unit, and updates contents of the tag verification information storage unit by storing the at least two acquired certification ID codes into the tag verification information storage unit as verification ID codes by priority.

Shinzaki discloses code that is correlated with levels that are equal to or higher than a threshold value (Shinzaki col. 12 lines 51-60 discloses that the password and biometrics of a user has to be equal to or larger than the threshold, then the user is authenticated).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono in view of Ogawa authentication apparatus that have

weight coefficients used to authenticate the user with values equal to or greater than a threshold value, as taught by Shinzaki. The combination of Ono in view of Ogawa and Shinzaki would yield to claim limitation "the predetermined type code is correlated with priority levels that are equal to or higher than a priority-level threshold value, and the update unit acquires at least two certification ID codes that have priority levels that are equal to or higher than the priority-level threshold value, from the plurality of certification ID codes received by the receiving unit, and updates contents of the tag verification information storage unit by storing the at least two acquired certification ID codes into the tag verification information storage unit as verification ID codes by priority".

The motivation would be to provide to users that have a poor reproducibility in biometric information with an enhanced feature to verify the user (Shinzaki col. 1 lines 62-67).

In regard to claim 11, Ono in view of Ogawa discloses the authentication apparatus of claim 8 further comprising a point storage unit (Ono fig. 3 & ¶0048 integrated into the authentication holding unit discloses as weight coefficient are summed up to authenticate a user) operable to store a plurality of point values (Ono fig. 3: weight coefficient column) with a plurality of type codes (Ono fig. 3: authentication information) corresponding thereto (Ono fig. 3: authentication information column corresponds to the weight coefficient column), wherein the predetermined type codes (Ono fig. 3: authentication information) are correlated with point values (Ono fig. 3: authentication information column corresponds to the weight coefficient column), and

the update unit (Ogawa fig. 4: 405) acquires at least two (Ogawa fig. 4: 405 & 403 & 0094 discloses the updating section receives the transformation result and presentation symbol string) certification ID codes (Ono fig. 3: authentication information & weight coefficients) that have point values(Ono fig. 3: weight coefficient column), from the plurality of certification ID codes received by the receiving unit (Ono ¶0036).

Ono in view of Ogawa does not disclose the predetermined type codes are correlated with point values are equal to or higher than a point-value threshold value, and the update unit acquires at least two certification ID codes that have point values that are equal to or higher than the point-value threshold value, from the plurality of certification ID codes received by the receiving unit, and updates contents of the tag verification information storage unit by storing the at least two acquired certification ID codes into the tag verification information storage unit as verification ID codes by priority.

Shinzaki discloses authentication apparatus that has values that are equal to or higher than a threshold value (Shinzaki col. 12 lines 51-60 discloses that the password and biometrics of a user has to be equal to or larger than the threshold and then the user is authenticated).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono in view of Ogawa authentication apparatus to include values that are equal to or higher than a threshold value, as taught by Shinzaki. The combination of Ono in view of Ogawa and Shinzaki would yield to the claim limitation "the predetermined type codes are correlated with point values are equal to or

higher than a point-value threshold value, and the update unit acquires at least two certification ID codes that have point values that are equal to or higher than the point-value threshold value, from the plurality of certification ID codes received by the receiving unit, and updates contents of the tag verification information storage unit by storing the at least two acquired certification ID codes into the tag verification information storage unit as verification ID codes by priority".

The motivation would be to provide to users that have a poor reproducibility in biometric information with an enhanced feature to verify the user (Shinzaki col. 1 lines 62-67).

In regard to claim 14, Ono in view of Ogawa discloses the authentication apparatus of claim 13.

Ono in view of Ogawa does not disclose an authentication apparatus comprising an identification information storage unit operable to store first identification information, a user judgment unit operable to receive second identification information and judge whether or not the first identification information matches the received second identification information, wherein the predetermined condition for update is that the first identification information matches the second identification information, and if the first identification information matches the second identification information, the update unit updates the contents of the tag verification information storage unit, and the transmission unit transmits, for each piece of authentication data for verification having been updated by the update unit, a piece of authentication data for verification as a

piece of authentication data for certification, to a wireless IC tag having an ID code corresponding to the piece of authentication data for verification.

Shinzaki discloses authentication apparatus comprising an identification information storage unit (Shinzaki fig. 6: discloses as password information registration and storage unit) operable to store first identification information (Shinzaki discloses as password col. 12 lines 1-2), a user judgment unit (Shinzaki fig. 6: password information matching check unit) operable to receive second identification information (Shinzaki fig. 6: 44 to 42) and judge whether or not the first identification information matches the received second identification information (Shinzaki fig. 7: S33 & col. 12 lines 2-5 & 46-50), where there was a condition set that the first identification information had to match the second identification information (Shinzaki col. 12 lines 2-5).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono in view of Ogawa authentication apparatus with the inclusion of an optional verification feature, as taught by Shinzaki. The combination of Ono in view of Ogawa and Shinzaki would yield to the claim limitation "an identification information storage unit operable to store first identification information, a user judgment unit operable to receive second identification information and judge whether or not the first identification information matches the received second identification information, wherein the predetermined condition for update is that the first identification information matches the second identification information, and if the first identification information matches the second identification information, the update unit updates the contents of the tag verification information storage unit, and the transmission unit transmits, for

each piece of authentication data for verification having been updated by the update unit, a piece of authentication data for verification as a piece of authentication data for certification, to a wireless IC tag having an ID code corresponding to the piece of authentication data for verification".

The motivation would be to provide to users that have a poor reproducibility in biometric information with an enhanced feature to verify the user (Shinzaki col. 1 lines 62-67).

5. Claims 7 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Ogawa (PG-Pub No. 2005/0027990 A1) and further in view of Nakajima (PG-Pub No. 2002/0108062 A1).

In regard to claim 7, Ono in view of Ogawa discloses the authentication apparatus of claim 5.

Ono in view Ogawa does not disclose the authentication apparatus comprising a distance calculating unit operable to calculate values of a distance between the authentication apparatus and each of the wireless IC tags from which the plurality of certification ID codes have been received, wherein the update unit acquires at least two certification ID codes for which calculated values of the distance are each equal to or lower than a predetermined value, from the plurality of received certification ID codes.

Nakajima discloses an authentication system comprising a distance calculating unit (Nakajima fig. 1: 70 discloses as a location matching server) operable to calculate values of a distance between a mobile station and credit card (Nakajima ¶0055-0056

discloses the location matching server is able to determine the if the mobile station (authentication apparatus) and credit card (wireless IC tag) are in the same location). Nakajima further discloses that the calculated values of the distance are each equal to or lower than a predetermined value (Nakajima ¶0074-0077 discloses the location server can determine if the mobile station and credit card are in the same area by determining if they are in the same radio cells).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono in view Ogawa authentication apparatus to include a distance calculating unit, as taught by Nakajima. The combination of Ono in view of Ogawa and Nakajima would yield to the claim limitation "a distance calculating unit operable to calculate values of a distance between the authentication apparatus and each of the wireless IC tags from which the plurality of certification ID codes have been received, wherein the update unit acquires at least two certification ID codes for which calculated values of the distance are each equal to or lower than a predetermined value, from the plurality of received certification ID codes".

The motivation would be to provide an additional feature of authentication of a user without imposing a burden on the user of the device (Nakajima ¶0273).

In regard to claim 15, Ono in view of Ogawa discloses the authentication apparatus of claim 13 wherein the update unit (Ogawa fig. 4: 405) acquires at least two pieces of data corresponding to ID codes among the received ID codes (Ogawa ¶0094

discloses updating section receives a transformation result and presentation symbol string).

Ono in view of Ogawa does not disclose the authentication apparatus further comprising a distance calculating unit operable to calculate values of a distance between the authentication apparatus and each of the wireless IC tags from which the plurality of ID codes have been received, wherein the update unit acquires at least two pieces of authentication data corresponding to ID codes for which calculated values of the distance are each equal to or lower than a predetermined value, among the plurality of received ID codes.

Nakajima discloses an authentication system comprising a distance calculating unit (Nakajima fig. 1: 70 discloses as a location matching server) operable to calculate values of a distance between the authentication apparatus (Ono fig. 1: 200) and each of the wireless IC tags (Nakajima ¶0055-0056 discloses the location matching server is able to determine if the mobile station (authentication apparatus) and credit card (wireless IC tag) are in the same location).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono in view of Ogawa authentication apparatus to provide a feature to determine the distance between the authentication apparatus and IC tag, as taught by Nakajima. The combination of Ono in view of Ogawa and Nakajima would yield to the claim limitation "the authentication apparatus further comprising a distance calculating unit operable to calculate values of a distance between the authentication apparatus and each of the wireless IC tags from which the plurality of ID

codes have been received, wherein the update unit acquires at least two pieces of authentication data corresponding to ID codes for which calculated values of the distance are each equal to or lower than a predetermined value, among the plurality of received ID codes".

The motivation would be to provide an additional feature of authentication of a user without imposing a burden on the user of the device (Nakajima ¶0273).

6. Claims 10 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Ogawa (PG-Pub No. 2005/0027990 A1) and further in view of Shinzaki (Pat. No. 7,007,298 B1) and further in view of Omae (PG-Pub No. 2006/0174121 A1).

In regard to claim 10, Ono in view of Ogawa and Shinzaki discloses the authentication apparatus of claim 9.

Ono in view of Ogawa and Shinzaki does not disclose the authentication apparatus comprising a priority level update unit operable to receive (Omae fig. 8: discloses as Device ID/Attribute Setting and Update Unit that is operable to receive a device ID, ¶0069) a type code (Ono fig. 3: authentication information) and a priority level (Ono fig. 4: Reference value), and update the priority level storage unit by replacing a priority level (Omae ¶0069 discloses that the Device ID/Attribute Setting and Update Unit can change the priority level of a device), which is stored in the priority level storage unit in correspondence with the received type code, with the received priority level.

Omae discloses security system that comprises a priority level update unit operable to receive (Omae fig. 8: discloses as Device ID/Attribute Setting and Update Unit that is operable to receive a device ID, ¶0069) and update external devices by replacing a priority level (Omae fig. 8: 2 & 3 & ¶0069 discloses that the Device ID/Attribute Setting and Update Unit can change the priority level of a device).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono in view of Ogawa and Shinzaki authentication apparatus to include a priority level update unit, as taught by Omae. The combination of Ono in view of Ogawa, Shinzaki and Omae would yield to the claim limitation "a priority level update unit operable to receive a type code, and update the priority level storage unit by replacing a priority level, which is stored in the priority level storage unit in correspondence with the received type code, with the received priority level".

The motivation would be to simplify management process of the group management server without reducing the security (Omae ¶0017).

In regard to claim 12, Ono in view of Ogawa and Shinzaki discloses the authentication apparatus of Claim 11.

Ono in view of Ogawa and Shinzaki does not disclose the authentication apparatus comprises a point update unit operable to receive a type code and a point value, and update the point storage unit by replacing a point value, which is stored in

the point storage unit in correspondence with the received type code, with the received point value.

Omae discloses an apparatus that comprises an update unit operable to receive a code (Omae fig. 8: discloses as Device ID/Attribute Setting and Update Unit that is operable to receive a device ID, ¶0069) and update a value (Omae ¶0069 discloses that the Device ID/Attribute Setting and Update Unit can change the value of a device). Although Omae may not disclose his device is used as a point update unit, it would have been obvious to replace Omae update unit in order to update a value of a device, there by increasing the security of the authentication device.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono in view of Ogawa and Shinzaki authentication apparatus with a update unit to bring up to date the values stored in the device, as taught by Omae. The combination of Ono in view of Ogawa, Shinzaki and Omae would yield to the claim limitation "a point update unit operable to receive a type code and a point value, and update the point storage unit by replacing a point value, which is stored in the point storage unit in correspondence with the received type code, with the received point value".

The motivation would be to simplify management process of the group management server without reducing the security (Omae ¶0017).

7. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Zhang (PG-Pub. No. 2004/0064698 A1).

In regard to claim 18, Ono discloses the authentication apparatus of claim 2 further comprising a control unit (Ono fig. 2: 230 & ¶0037 discloses as a personal authentication unit) operable to control the receiving unit (Ono fig. 2: 230) to receive the plurality of pieces of tag certification information (Ono ¶0046 discloses the personal authentication system is the element that reads controls the transmit signal that is sent to the IC tags).

Ono does not disclose the authentication apparatus of claim 2, wherein the tag verification information storage unit further stores expiration date/time information that indicates an expiration date/time of each piece of tag verification information, and the authentication apparatus further comprises a control unit operable to, if having judged that any expiration date/time of the plurality of pieces of tag verification information has not been reached, control the receiving unit to receive the plurality of pieces of tag certification information.

Zhang discloses an authentication system that stores expiration date/time information that indicates an expiration date/time of access to the device (Zhang ¶0223 discloses that the apparatus can store a date or time of expiration in which a user has access to a device).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono authentication apparatus to associate an expiration time or date with information received by the authentication apparatus, as taught by Zhang. The combination of Ono in view of Zhang would yield to the claim limitation "the tag verification information storage unit further stores expiration date/time information

that indicates an expiration date/time of each piece of tag verification information, and the authentication apparatus further comprises a control unit operable to, if having judged that any expiration date/time of the plurality of pieces of tag verification information has not been reached, control the receiving unit to receive the plurality of pieces of tag certification information".

The motivation would be to provide the user with an additional feature, for example, by associating expiration date or time with the information transmitted to the device this would increase the security level for the user.

8. Claims 23 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1).

In regard to claim 23, claim 23 is directed toward embody the method of claim 22 in a "program".

Ono does not disclose an authentication program for an authentication apparatus which permits a user to use a function provided by the authentication apparatus if authenticity of the user is certified by authentication.

It would have been obvious to embody the procedures of Ono discussed with respect to claim 22 in a "program" in order that the instructions could be automatically performed by a processor.

In regard to claim 24, claim 24 is directed toward embody the method of claim 22 in a "computer readable medium".

Ono does not disclose a computer-readable recording medium recording therein an authentication program that causes a computer to operate as an authentication apparatus which permits a user to use a function provided by the authentication apparatus if authenticity of the user is certified by authentication.

It would have been obvious to embody the procedures of Ono discussed with respect to claim 22 in a "computer readable medium" in order that the instructions could be automatically performed by a processor.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CURTIS KING whose telephone number is (571)270-5160. The examiner can normally be reached on Mon-Thurs 7:30 - 6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hai Tran can be reached on (571)272-7305. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ck/
08/03/2009
/Hai Tran/
Supervisory Patent Examiner, Art Unit 4147